F-Secure Mobile Security for Android Ver.8

ユーザーズガイド

目次

第
1
章

インストール

トピック ：

ここでは、F-Secure Mobile Security をモバイルのデバイスにインストールするための方法を説明します。
製品をデバイスにインストールする方法を選択します。
- インストーラをコンピュータにダウンロードして、デバイスに転送する
- インストーラをデバイスに直接ダウンロードする

F-Secure Mobile Security のインストール後、ライセンスを認証してください。ライセンスを認証したら、デバイスは保護されます。

インストール

Mobile Security をモバイルデバイスにインストールする方法について説明します。

Mobile Security を旧バージョンからアップグレードする場合、旧バージョンをアンインストールする必要はありません。アップグレード後、Mobile Security の設定が正しく継承されていることを確認してください。

Mobile Security をインストールするには

1. 設定 > アプリケーション の順に選択して、[提供元不明のアプリ] が有効になっていることを確認します。
   この設定が有効な場合、Android Market 以外のアプリケーションをインストールできるようになります。
2. インストーラをコンピュータにダウンロードして、デバイスに転送します。または、インストーラをデバイスに直接ダウンロードします。詳細については、デバイスの取扱説明書を参照してください。
3. デバイスでインストーラを実行します。
   メモリカードからインストーラを実行する場合、サードパーティのファイルマネージャが必要になります。
   Mobile Security がデバイスにインストールされます。
4. インストール後、[開く] を選択して、アプリケーションを認証します。

Mobile Security を認証しない限り、デバイスは保護されません。

認証

ライセンスを認証すると、デバイスに対する保護が有効になります。

ライセンスを認証するには

1. F-Secure Mobile Security を起動します。
   ライセンスの使用許諾契約書が表示されます。
2. 内容を確認し、同意する場合、[OK] を選択します。
   ライセンスの認証手続きが始まります。
3. 最初に「評価版」でインストールを完了します。
   インストーラをダウンロード後、評価版でのインストールが完了します。
   その後、詳細 > ライセンスの順に選択します。
   「キーコードをお持ちですか？」をクリックし、製品版ライセンスキーコードを入力します。
4. [認証] を選択します。

   注:　認証中に Mobile Security はエフセキュアの更新サービスに接続します。

認証後、製品の機能を設定できるウィザードが開きます。

なお、アンチセフトを利用するためにデバイス管理者を有効にする必要があります。

F-Secure Mobile Security を設定する

F-Secure Mobile Security を使用する前に製品の設定を行う必要があります。

次の方法でアンチセフト、ペアレンタルコントロール、連絡先フィルタを有効にできます。

1. セキュリティコードを作成します。

   注: セキュリティコードを後で変更するには、設定 > 一般設定を開き、［セキュリティコードを設定］を選択します。

   アンチセフトのリモート機能とペアレンタルコントロールを利用するにはセキュリティコードが必要となります。

2. デバイスの管理を行うための認証を行います。デバイス管理者を認証するために［認証］を選択します。
3. デバイスのスクリーンロックを設定していない場合、スクリーンロックを設定します。

   詳細については、デバイスの取扱説明書を参照してください。

4. 信頼済みの電話番号を入力します。

   デバイスの SIM カードが変更されたときに信頼済みの電話番号に通知が送信されます。

5. ペアレンタルコントロールを設定するためにデバイスを利用するユーザの年齢層を選択します。

アンチセフトとペアレンタルコントロールを設定したら本製品が有効になります。

F-Secure Mobile Security を Android デバイスからアンインストールする

デバイスから F-Secure Mobile Security をアンインストールする方法について説明します。

F-Secure Mobile Security をアンインストールするには

1. メインビューで［詳細］を選択します。
2. 「詳細」メニューから［バージョン情報］を選択します。
3. ［アンインストール］を選択します。

   アンチセフトのセキュリティコードを作成した場合、アンインストールを行うためにセキュリティコードを入力する必要があります。

F-Secure Mobile Security がデバイスから削除されます。

注: 「デバイス管理者」の一覧で本製品が無効になります。アンインストールをキャンセルすると、製品をもう一度認証する必要があります。

第

2

章

データの保護をする

トピック ：

・リモートアンチセフトを有効にする

・SMS 警告

・位置情報を共有するアンチセフトのアラームを使用

アンチセフトを使用すると、デバイスを紛失した場合でもデバイスの本体とデータを保護することができます。

デバイスを紛失しても、デバイスに SMS を送ることでデバイスをロックすることが可能です

・一度デバイスをロックすると、アンロックパターンを利用しない限り、デバイスのロックを解除することはできません。

注: 「リモートロック」を使用するには、デバイスのアンロックパターンを有効にする必要があります。

・一度デバイスをロックすると、セキュリティコードを利用しない限り、デバイスのロックを解除することはできません。

「リモート削除」は、デバイスのデータをリモートから削除する機能です。

・デバイスにリモート削除を指定する SMS を送ると、デバイスのデータ（SD カード、SMS/MMS メッセージ、連絡先、カレンダーの各データ）が削除されます。リモート削除を行う場合、セキュリティのためにGoogle アカウントをパスワードを変更することを推奨します。

・リモート削除の SMS をデバイスに送るときにデバイスの全設定が初期化されます。

リモートアンチセフトを有効にする

リモートアンチセフトを有効にすると、デバイスに SMS を送ることでデバイスのロックまたはデータの削除を行うことが可能になります。

リモートアンチセフト設定するには
1. メインビューで［アンチセフト］を選択します。
2. 「アンチセフト」メニューから［有効］を選択します。
3. スクリーンロックを設定します。
4. セキュリティコードを設定します。
5. 「信頼済みの番号（携帯電話）」を入力します。これは後でも設定可能です。

アンチセフトが有効になります。

リモートロック

「リモートロック」は、デバイスをリモートからロックして、第三者がデバイスを使用することを阻止します。

デバイスをリモートからロックするには
1. 次の内容を持った SMS を「信頼済みの番号」からデバイスに送ることでデバイスをロックできます。
   #LOCK#〈セキュリティコード〉（例：#LOCK#12345678）
2. デバイスをロックすると、ロック SMS を送信した電話へ返信メッセージが送られます。

一度デバイスをロックすると、設定したスクリーンロックを利用しない限り、デバイスのロックを解除することはできません。

リモート削除

「リモート削除」は、デバイスのデータをリモートから削除して、第三者がデバイスのデータを使用することを阻止します。

リモートからデバイスのデータを削除するには
1. 次の内容を持った SMS を「信頼済みの番号」からデバイスに送ることでデバイスのデータを削除できます。
   #WIPE#〈セキュリティコード〉（例：#WIPE#12345678）
2. リモート削除を行うと、SMS を送信した電話へ返信メッセージが送られます。

リモート削除を行うと、SD カード、SMS/MMS メッセージ、連絡先、カレンダーの各データが削除されます。また、リモート削除の SMS をデバイスに送るときにデバイスの全設定が初期化されます。

リモートロケート

デバイスを見失った場合、デバイスに SMS を送ることでデバイスの位置を検索することが可能です。

注: デバイスの位置情報を検索するには、デバイスの GPS 機能が有効になっている必要があります。

デバイスの位置を検索するには

次の内容を持った SMS を「信頼済みの番号」からデバイスに送ることでデバイスの位置を検索できます。

#LOCATE#<セキュリティコード>（例: #LOCATE#12345678）

しばらくしてからデバイスの位置を知らせる SMS が届きます。

ヒント: 本製品をデバイスにはじめて設定するときには、リモートロケート機能の動作を確認するためにロケート用の SMS を検証用に送ることを推奨します。

注: アンチセフトは SMS を通じてデバイスの位置データを送りますが、そのデータを保存することはありません。

SMS 警告

アンチセフトは、デバイスの SIM カードが変更された場合に SMS を別のデバイスに送る「SMS 警告」機能を搭載しています。

SMS 警告を有効にするには

1. メインビューで［アンチセフト］を選択します。
2. 「アンチセフト」メニューから［設定］を選択します。
3. ［信頼済みの番号］を選択します。

   「信頼済みの番号」を設定する画面が開きます。
4. SIM カード変更時に送る SMS の送信先（電話番号）を指定します。

SMS 警告が有効になります。

アンチセフトのアラームを使用する

デバイスの紛失や盗難時にアラーム（警告音）を鳴らすことができます。

アラームを設定するには

1. 次の内容を持った SMS を「信頼済みの番号」からデバイスに送ることでアラームを再生できます。

   #ALARM#<セキュリティコード>#<再生回数> （例: #ALARM#12345678#3）

   注: 再生回数でアラームを鳴らす回数を指定できます（指定しなくてもアラームは鳴ります）。
2. SMS を受信すると、デバイスがロックされ、アラームが鳴ります。SMS を送信した電話へ返信メッセージが送られます。

設定したスクリーンロックを利用することでアラームを無効にできます。

ヒント:次の内容を持った SMS を「信頼済みの番号」からデバイスに送ることでアラームをリモートから停止する事もできます。#ALARM#<セキュリティコード>#0

第
3
章

ブラウザ保護

トピック：

- ブラウザ保護を使用する
- インターネットを安全に利用する

ここでは、ブラウザ保護（セーフブラウザ）の機能について説明します。ブラウザ保護は個人情報（クレジットカード情報、ユーザアカウント情報、パスワードなど）を盗む Web サイトからユーザを保護します。

ブラウザ保護を有効にする

ブラウザ保護を設定するには

1. メインビューで［セーフブラウザ］を選択します。
2. ［有効］を選択します。

ブラウザ保護を有効にすると、危険な Web サイトがブロックされるようになります。［戻る］を選択すると、前の画面に戻れます。

ブロックした Web ページで表示される［Web ページにアクセスする］リンクをクリックすると、ブロックしたページにアクセスすることが可能です。

ブラウザ保護を使用する

ブラウザ保護を活用するには Safe Browser を使用する必要があります。他のブラウザではブラウザ保護は機能しません。

次の方法でブラウザ保護をブラウザで利用できます。

ブラウザを起動するには

･本製品の専用ブラウザ(セーフブラウザ)を開きます。メインビューで、［セーフ ブラウザ］のオプションから［ブラウザを起動する］を選択します。

･Android のランチャーから［Safe Browser］を開きます。

インターネットを安全に利用する

ブラウザ保護を使用すると、危険性のある Web サイトにアクセスすることを防ぐことができます。

Web ページにアクセスする際に Web ページの安全性が自動的に確認されます。アクセスしようとしている Web ページが「不審」または「危険」と評価されている場合、Web ページのアクセスがブロックされます。

Web ページの評価は、エフセキュアのマルウェア分析やパートナーからの調査などに基づいています。

第

4

章

ウイルスをスキャンする

トピック：

- マニュアル スキャン
- 感染したファイルの処理
- スケジュール スキャン

F-Secure Mobile Security はデバイスに対してウイルスと悪質なコンテンツのスキャンを行います。

F-Secure Mobile Security は、インストール済みのプログラムおよびデバイスに装着されているメモリーカードに対してウイルス、スパイウェア、リスクウェアのスキャンを行います。

注： F-Secure Mobile Security がデバイスをスキャンするよう警告を表示したときにはスキャンを実行することを推奨します。

マニュアル スキャン

必要に応じて、手動でウイルスのスキャンを実行することができます。

手動でスキャンを実行するには

1. メインビューで［アンチウィルス］を選択します。
2. ［スキャンする］を選択します。

   ウイルススキャンが開始します。
3. スキャンが完了したら、次の情報が表示されます。

   ･感染 – 検出された感染の数を示します。

   ･不要な可能性のあるアプリ- 長い間使用されていないアプリの数
4. ［OK］を選択してスキャンを終了します。

感染したアプリケーションやファイルが検出されたら、デバイスから削除することを推奨します。

感染したファイルの処理

特定のファイルに感染が検出された場合、感染したファイルをデバイスから削除することができます。

感染したファイルを処理するには

1. メインビューで［アンチウィルス］を選択します。
2. ［感染したファイル］を選択します。

   感染したファイルの一覧が表示されます。
3. 処理するファイルを選択します。
4. 感染したファイルを選択すると、ファイルの詳細を確認できます。「感染の詳細」画面では、感染したファイルのパスと名前、および感染の原因となるウイルス名が表示されます。
5. ［削除］または［アンインストール］を選択すると、感染したファイル/アプリケーションを取り除きます。

ウイルス、トロイの木馬、ワーム、その他のマルウェアに関する追加/詳細情報は、エフセキュアの Web サイト（*http://www.f-secure.com/virus-info/*）でご覧になれます。

スケジュールスキャンを設定する

定期的にスキャンするようにスケジュールが設定できます。

スケジュールスキャンを設定するには

1. メインビューで［アンチウィルス］を選択します。
2. ［設定］を選択します。
3. 「スケジュールスキャンを有効にする」にチェックを入れスキャン間隔・スキャン時間を設定します。

第

5

章

お子様/未成年に安全なインターネット環境を設定する

トピック：

- ユーザプロフィール
- ユーザプロフィールを指定する
- アプリケーション通信制御を使用する。

ペアレンタルコントロールはお子様/未成年がインターネット上の望ましくないコンテンツにアクセスすることを阻止します。
インターネットには数多くの面白い Web サイトがある反面、お子様や未成年に危険性があるのも事実です。お子様/未成年のユーザはモバイルデバイスを利用してインターネットにアクセスすることが一般的になっており、ほとんどの場合その行動は監視されていません。多くの Web サイトにはお子様や未成年に対して望ましくないコンテンツが含まれているため、お子様/未成年がそのようなコンテンツさらされてしまうことは簡単です。また、ウイルスなどの不正なファイルを誤ってダウンロードしたり、嫌がらせのメールを配信されたりすることも可能です。
ペアレンタルコントロールを利用することで、お子様/未成年のユーザが不正なコンテンツにアクセスすることを制限できます。

ユーザプロフィール

「ユーザプロフィール」を利用して、ティーンエイジャとチャイルドプロフィールのユーザがアクセスできる Web サイトのカテゴリを指定することができます。

ペアレンタルコントロールはユーザがアクセスしようとする Web ページを分析し、コンテンツに基づいて望ましくない Web ページをブロックします。

ペアレンタルコントロールには異なるコンテンツを制限するプリセットのプロフィールが 3 つ搭載されています。「ティーンエイジャ」プロフィールは一部のコンテンツに対するアクセスを制限し、「チャイルド」プロフィールにはより厳しい制限が適用されます。「成人」プロフィールのユーザはインターネットを制限なくアクセスできます。

ユーザプロフィールはインストール時に、またはペアレンタルコントロールの設定ページで後から設定することができます。

コンテンツタイプ

ペアレンタルコントロールを使用して、コンテンツ別に Web サイトのアクセスをブロックすることができます。

- アダルト
  性的な表現や性描写を含む成人向けのコンテンツを示します。アダルトショップやヌードなどの性的コンテンツ。
- チャット
  Web ベースのチャットプログラムやインスタントメッセージ用ソフト、チャットサイトなど。
- Web メール
  メールアカウントを作成できるサイトやブラウザを通じてメールを送受信できるサイトなど。
- 武器
  武器の写真や説明、爆弾の作り方を含むサイトなど。
- ギャンブル
  オンラインカジノ、ギャンブル関連の Web サイトなど。
- 麻薬
  薬物使用を促すサイト。麻薬の栽培や売買に関する情報を含むサイトなど。
- 出会い系
  出会い系やメールオーダーブライドのサイトなど。
- ソーシャルネットワーク
  プライベートやビジネスの交流に関する社会的ネットワークを提供するサイトなど。
- 掲示板
  コメントを表示/投稿できるオンライングループや掲示板を作成できるプログラムなど。
- ブログ
  オンラインの日記や個人 Web ページ、ブログ、ポッドキャストなど。
- ショッピングとオークション
  Web 上で商品を直接注文できるサイトや価格比較、インターネットのオークションサイトなど。
- カルト
  宗教、その他のイデオロギーに反対する熱狂的なグループを支援するサイトなど。

· お酒とタバコ

お酒やタバコに関する製品の情報を提供、促進、支援するサイトなど。

· 憎悪表現と暴力

特定の宗教、人種、民族、性別、年齢層、障害者、性的指向に対する差別を示すサイト、または暴力、動物虐待、機関への破壊行為に関する写真や説明を含むサイトなど。

· 違法ダウンロード

プログラムの違法/不審なアクセスを提供するサイト、またはネットワークやシステムに問題を発生させるプログラムを開発および配布するサイトなど。

· アノニマイザー

インターネットの行動を追跡できないようにするサイトやフィルタを回避する情報を提供するサイトなど。

· 不明

コンテンツが認識されないサイトは、「不明」のカテゴリとして指定されます。

ユーザプロフィールを指定する

ユーザプロフィールを利用して、デバイスのユーザを指定することができます。ペアレンタルコントロールはプロフィールに基づいて Web コンテンツを制限します。

ユーザプロフィールを変更するには

1. メインビューで［ペアレンタルコントロール］を選択します。
2. ［有効］を選択します。、
3. ［年齢層］でユーザプロフィールを指定します。
   年齢層によって、ユーザがアクセスできるカテゴリが異なります。
5. ［設定］>［Web アクセス］で、カテゴリを表示/編集できます。
6. 許可するカテゴリを指定します。

年齢層/ユーザプロフィールを変更すると、Web ページのアクセスは、ペアレンタルコントロールが許可したページに限定されます。

「許可したアプリケーション」を使用する

「許可したアプリケーション」を使用して、アプリケーションの制限とアンインストールを行うことができます。「許可したアプリケーション」を使用するにはペアレンタルコントロールを有効にします。

「許可したアプリケーション」を使用するには

1. メインビューで［ペアレンタルコントロール］を選択します。
2. ［設定］>［許可したアプリケーション］で、インストールされているアプリケーションの一覧が表示されます。
3. アプリケーションの使用を許可する場合、アプリケーションの横にあるチェックボックスをオンにしてください。チェックボックスをオフにすると、アプリケーションが制限されます。デフォルトではペアレンタルコントロールは全アプリケーションのアクセスを許可します。

制限したアプリケーションを起動しようとすると、アプリケーションがブロックされていることを示すページが表示され、アプリケーションのアクセスがブロックされます。

第
6
章

特定の電話番号からの着信とメールを拒否する

トピック：

- 連絡先フイルタ
- ﾌﾞﾛｯｸした着信とﾒｯｾｰｼﾞを確認

連絡先フィルタを有効にすると、特定の電話番号からの着信とメールを拒否することができます。
連絡先フィルタを使用して、望ましくない電話や迷惑メールをブロックできます。
着信と SMS/MMS メッセージのブロック対象となる電話番号を指定することができます。ブロックした電話番号に電話をかけることも禁止されます

連絡先フィルタ

連絡先フィルタは、特定の電話番号からの着信とメッセージを拒否する機能です。

特定の電話番号からの着信とメッセージを拒否するには

1. メインビューで［連絡先フィルタ］>［設定］を選択します。
2. ［ブロックリスト］を選択します。
   セキュリティコードを設定します(設定していない場合)。
3. ブロック対象の名前と電話番号を入力します。
4. ［保存］を選択して、指定の電話番号をブロック対象に設定します。

連絡先フィルタを有効にすると、ブロックされている電話番号からの着信とメッセージが拒否され、発信も禁止されます。

ブロックした着信とメッセージを確認する

連絡先フィルタのブロック履歴で拒否した着信とメッセージを確認することができます。

連絡先フィルタのブロック履歴を表示するには

1. メインビューで［連絡先フィルタ］>［設定］を選択します。
2. ［ブロック履歴］を選択します。
3. 拒否した電話番号等が表示されます。

第
7
章

F-Secure Mobile Security を更新する

トピック：

- 更新モードを選択する
- 手動更新

F-Secure Mobile Security の「自動更新」機能は、ウイルスの定義ファイルやプログラム本体を自動的に更新する機能です。

F-Secure Mobile Security を認証した時点で自動更新が有効になります。自動更新はインターネットに接続している際に更新を確認し、更新がある場合には更新をダウンロードします。

注： F-Secure Mobile Security の自動更新機能は有効なライセンスを必要とします。

更新モードを選択する

F-Secure Mobile Security をインストールしたら自動更新が有効になります。自動更新またはリアルタイムスキャンを無効にした場合、更新を手動で行う必要があります。

更新モードを選択するには

自動更新のモードを選択します。

- マイプロバイダ - デバイスがホームネットワークに接続している場合、更新を自動的にダウンロードします。
- 全プロバイダ - 更新を定期的にダウンロードして、ウイルス定義ファイルを最新の状態にします。
- 無効 - ウイルス定義ファイルを自動的に更新しないようにします。自動更新を無効にすることは推奨しません。

手動更新

Mobile Security を手動で更新することもできます。

更新を手動で確認するには

1. メインメニューで［詳細］>［更新］を選択します。

   更新を確認するにはインターネットの接続が必要です。

2. ［更新］を選択します。

   新しい更新が利用できる場合、ダウンロードの確認が表示されます。

3. ［はい］を選択して、更新をダウンロードします。
4. ダウンロードが完了したら、［インストール］を選択します。